BD

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-251295

(43)Date of publication of application : 14.09.2001

(51)Int.Cl. H04L 9/32
G06T 7/00

(21)Application number : 2000-057789

(22)Date of filing : 02.03.2000

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

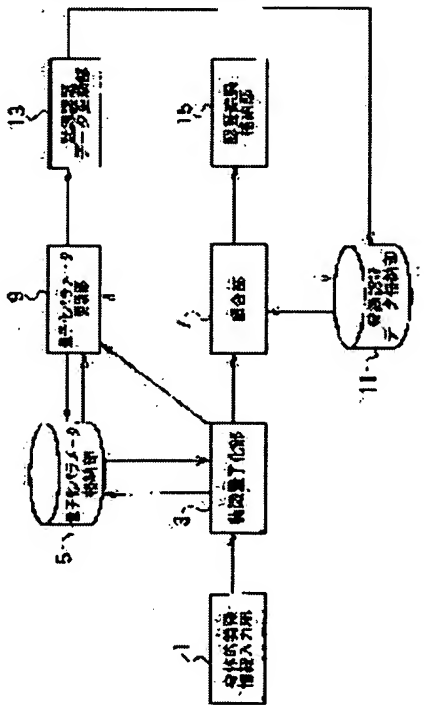
(72)Inventor : KADOGOE KAZUYA
KIMURA YOSHIMASA
TOMONO AKIRA
WAKAHARA TORU
SAKAMURA TAKESHI

(54) PERSONAL IDENTIFICATION METHOD AND SYSTEM, SERVER AND TERMINAL

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a personal identification method and device with high security and convenience for reducing the risk of any illicit identification due to the robbery of registered identification data as much as possible regardlessly of the unnecessity of any encipherment operation, key keeping and management work.

SOLUTION: A featured value obtained from physical characteristic information is quantized and converted into a quantized characteristic code, and unidirectional function value data generated by applying unidirectional functions to the quantized characteristic code string are stored as registered identification data. When physical characteristic information is newly inputted, the collation of identification confirmation data (unidirectional function value data) obtained by integrating quantized characteristic codes generated by adding perturbation to the quantized characteristic codes as necessary into unidirectional function values with the registered identification data is repeated only by the prescribed number of times while the parameter of the perturbation is changed, and when any unidirectional function value data matched with the registered identification data are found, it is judged that the data belong to the person himself who registered.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－251295
(P2001－251295A)
(43)公開日　平成13年９月14日(2001.9.14)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
H04L 9/32		H04L 9/00	675A	5B043
G06T 7/00		G06F 15/62	465A	5J104
			465P	
		H04L 9/00	673D	

審査請求 未請求 請求項の数22 ＯＬ （全 19 頁）

(21)出願番号　特願2000－57789(P2000－57789)

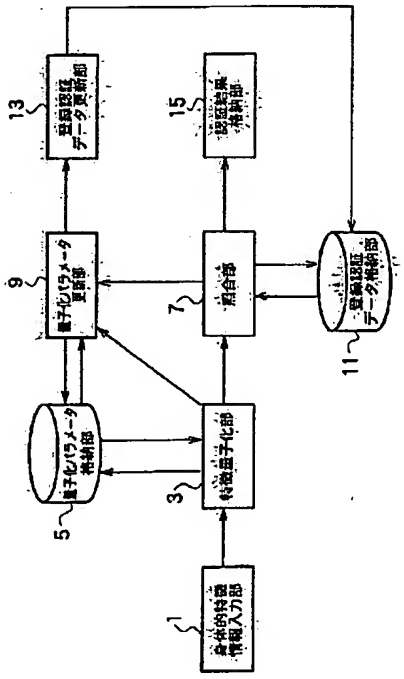
(22)出願日　平成12年３月２日(2000.3.2)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　角越　和也
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　木村　義政
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　個人認証方法及びその装置とサーバと端末

(57)【要約】
【課題】　暗号化操作や鍵の保管・管理業務が不要であるにも関わらず、登録認証データの盗難による不正な認証の危険性を極力抑えることができる個人認証、つまり、高い安全性及び利便性を有する個人認証方法及びその装置とサーバと端末を提供する。
【解決手段】　身体的特徴情報から得られる特徴量に量子化操作を施して量子化特徴コードに変換し、該量子化特徴コードの列に一方向性関数を施して生成される一方向性関数値データを登録認証データとして格納しておき、新たに身体的特徴情報が入力されると、その量子化特徴コードに適宜摂動を加えて生成した量子化特徴コードを一方向性関数値化した認証確認データ（一方向性関数値データ）と、上記登録認証データとの照合を上記摂動のパラメータを変えながら所定の回数だけ反復して行い、上記登録認証データに一致する上記一方向性関数値データが見い出された場合には登録した本人のものであると判定する。



1

【特許請求の範囲】

【請求項１】　身体的特徴量を用いて本人の認証を行う個人認証方法において、

個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成し、

該量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成し、

該一方向性関数値データと本人確認のために予め用意された登録認証データとを照合し、

該一方向性関数値データと登録認証データとが一致した場合には該登録認証データに対応する本人であると判定し、

該一方向性関数値データと該登録認証データとが不一致の場合には、前記身体的特徴量と量子化特徴コード列のいずれかに摂動を行い新たな一方向性関数値データを生成すること及びこの生成された一方向性関数値データと前記登録認証データとを照合することとを繰り返し、

所定回数内の照合により、該一方向性関数値データと登録認証データとが一致した場合には該登録認証データに対応する本人であると判定し、

所定回数内の照合で一致しない場合、該登録認証データに対応する本人ではないと判定することを特徴とする個人認証方法。

【請求項２】　身体的特徴量を用いて本人の認証を行う個人認証方法において、

認証すべき個人の身体的特徴を取得して、当該身体的特徴の各特徴量に基づき量子化パラメータを求め、

該量子化パラメータと前記各特徴量に基づき量子化特徴コードを生成し該量子化特徴コードの列を一方向性関数によって一方向性関数値データに変換して登録認証データとすることを特徴とする請求項１に記載の個人認証方法。

【請求項３】　身体的特徴量を用いて本人の認証を行う個人認証方法において、

個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成し、

該量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成し、

該一方向性関数値データと本人確認のために予め用意された登録認証データとを照合し、

該一方向性関数値データと登録認証データとが一致した場合には該登録認証データに対応する本人であると判定すると共に、該一方向性関数値データに対応する量子化特徴コード列に基づいて個人鍵を生成し、

該一方向性関数値データと該登録認証データとが不一致の場合には、前記身体的特徴量と量子化特徴コード列のいずれかに摂動を行い新たな一方向性関数値データを生成すること及びこの生成された一方向性関数値データと前記登録認証データとを照合することとを繰り返し、

該登録認証データに対応する本人であると判定された際

2

に、照合で一致した一方向性関数値データに対応する量子化特徴コード列に基づいて個人鍵を生成することを特徴とする個人認証方法。

【請求項４】　与えられた最大認証時間に基づいて、前記照合の最大回数を設定することを特徴とする請求項１乃至請求項３のいずれか１項に記載の請求項１に記載の個人認証方法。

【請求項５】　前記量子化する際のパラメータは、各特徴量の分布と与えられた最高本人拒否率と最大照合回数に基づいて設定されることを特徴とする請求項１乃至請求項４のいずれか１項に記載の個人認証方法。

【請求項６】　前記量子化する際のパラメータ中に擬似パラメータを含むことを特徴とする請求項１乃至請求項５のいずれか１項に記載の個人認証方法。

【請求項７】　前記照合によって一方向性関数値データと登録認証データとが一致したときに、取得した身体的特徴の特徴量を加味して新たな特徴量の分布を求め、その新たな特徴量の分布に基づき、量子化する際のパラメータを更新すると共に、当該新たなパラメータに基づき登録されている登録認証データの更新を行うことを特徴とする請求項１乃至請求項５のいずれか１項に記載の個人認証方法。

【請求項８】　前記身体的特徴量として、筆記具が筆記対象物に接触してから離れるまでをストロークと認識し、各ストロークの筆記時間を使うことを特徴とする請求項１乃至請求項７のいずれか１項に記載の個人認証方法。

【請求項９】　前記身体的特徴量として、筆記具が筆記対象物に接触してから離れるまでをストロークと認識し、取得された各ストロークを用い、該ストロークと、予め決められた複数の基本ストロークに最も類似する１又は２以上の上記基本ストロークのストローク番号を上記ストロークに対応する量子化特徴コードとして使用することを特徴とする請求項１乃至請求項８のいずれか１項に記載の個人認証方法。

【請求項１０】　複数の筆跡情報からストローク情報を抽出する際に、該筆跡情報間のストローク数の変動を吸収し、全データのストローク数を等しくした後に得られた各ストロークの筆記時間を身体的特徴量として用いて登録認証データを作成することを特徴とする請求項８または請求項９に記載の個人認証方法。

【請求項１１】　身体的特徴量を用いて本人の認証を行う個人認証装置において、

個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成する特徴量子化手段と、

該量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成する一方向性関数値化手段と、

該一方向性関数値データと本人確認のために予め用意された登録認証データとを照合する照合手段と、

該一方向性関数値データと該登録認証データとが不一致の場合には、前記身体的特徴量及び量子化特徴コード列のいずれかに摂動を行い新たな一方向性関数値データを生成すること及びこの生成された一方向性関数値データと前記登録認証データとを照合することとを繰り返す探索手段と、

前記探索手段において、当該照合回数が所定回数に達しても一致しなかった場合には該登録認証データに対応する本人ではないと判定して認証処理を終了をする認証棄却手段とを有することを特徴とする個人認証装置。

【請求項１２】　身体的特徴量を用いて本人の認証を行う個人認証装置において、

認証すべき個人の身体的特徴を取得して、当該身体的特徴の各特徴量に基づき量子化する際のパラメータを求める量子化パラメータ設定手段と、

前記量子化パラメータと前記各特徴量に基づき量子化特徴コードを生成し該量子化特徴コードの列を一方向性関数によって一方向性関数値データに変換して登録認証データとして登録認証データ格納部に登録する登録処理手段とを備えることを特徴とする個人認証装置。

【請求項１３】　身体的特徴量を用いて本人の認証を行う個人認証装置において、

個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成する特徴量子化手段と、

該量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成する一方向性関数値化手段と、

該一方向性関数値データと本人確認のために予め用意された登録認証データとを照合する照合手段と、

該一方向性関数値データと登録認証データとが一致した場合には該登録認証データに対応する本人であるか否かを判定する判定手段と、

該判定手段で本人であることが認証されたときには該一方向性関数値データに対応する量子化特徴コード列に基づいて個人鍵を生成する鍵生成手段と、

該一方向性関数値データと該登録認証データとが不一致の場合には、前記身体的特徴量と量子化特徴コード列のいずれかに摂動を行い新たな一方向性関数値データを生成すること及びこの生成された一方向性関数値データと前記登録認証データとを照合することとを繰り返す探索手段と、

一致しない場合、前記摂動と照合を繰り返して照合回数が所定回数に達した場合には該登録認証データに対応する本人ではないと判定して認証処理を終了する認証棄却手段とを有することを特徴とする個人認証装置。

【請求項１４】　与えられた最大認証時間に基づいて、前記照合の最大回数を設定することを特徴とする請求項１１乃至請求項１３のいずれか１項に記載の個人認証装置。

【請求項１５】　前記量子化する際のパラメータは、各

特徴量の分布と与えられた最高本人拒否率と最大照合回数に基づいて設定されることを特徴とする請求項１１乃至請求項１４のいずれか１項に記載の個人認証装置。

【請求項１６】　前記量子化する際のパラメータ中に、擬似パラメータを含むことを特徴とする請求項１１乃至請求項１５のいずれか１項に記載の個人認証装置。

【請求項１７】　前記照合手段において、一方向性関数値データと登録認証データとが一致したときに、取得した身体的特徴の特徴量を加味して新たな特徴量の分布を求め、その新たな特徴量の分布に基づき、量子化する際のパラメータを更新すると共に、当該新たなパラメータに基づき登録されている登録認証データの更新を行うことを特徴とする請求項１１乃至請求項１６のいずれか１項に記載の個人認証装置。

【請求項１８】　前記身体的特徴として、筆記具が筆記対象物に接触してから離れるまでをストロークと認識し、各ストロークの筆記時間を使うことを特徴とする請求項１１乃至請求項１７のいずれか１項に記載の個人認証装置。

【請求項１９】　前記身体的特徴量として、筆記具が筆記対象物に接触してから離れるまでをストロークと認識し、取得された各ストロークを用い、該ストロークと、予め決められた複数の基本ストロークに最も類似する１又は２以上の上記基本ストロークのストローク番号を上記ストロークに対応する量子化特徴コードとして使用することを特徴とする請求項１１乃至請求項１８のいずれか１項に記載の個人認証装置。

【請求項２０】　複数の筆跡情報からストローク情報を抽出する際に、該筆跡情報間のストローク数の変動を吸収し、全データのストローク数を等しくした後に得られた各ストロークの筆記時間を身体的特徴量として用いて登録認証データを作成することを特徴とする請求項１８または請求項１９に記載の個人認証装置。

【請求項２１】　身体的特徴量を用いて本人の認証を行う個人認証のための個人認証サーバにおいて、

本人確認のために予め用意された登録認証データを格納する登録認証データ格納手段と、

個人の少なくとも１種類の身体的特徴量を量子化して得られる量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成する一方向性関数値化手段と、

該一方向性関数値データと前記登録認証データ格納部に格納される登録認証データとを照合する照合手段とを有することを特徴とする個人認証サーバ。

【請求項２２】　身体的特徴量を用いて本人の認証を行う個人認証のための個人認証端末において、個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成する特徴量子化手段と、

該量子化特徴コード列を送信する送信手段とを有することを特徴とする個人認証端末。

5

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、身体的特徴に基づく個人認証方法及びその装置とサーバと端末に関する。

【０００２】

【従来の技術】情報化社会においてはセキュリティの確保が必要とされており、本人確認のために個人認証技術が重要となってきている。個人認証の手段としてパスワードによる認証方法もあるが、パスワードは盗用により他人が本人になりすますことができるという欠点、または、本人がパスワードを忘却する可能性があるという欠点がある。

【０００３】これを防止するため、本人固有の特徴である指紋や筆跡等の身体的特徴（バイオメトリクス）を認証に用いる方法がある。この方法は、本人の身体的特徴情報を登録認証データとして予め登録しておき、認証の際は、照合すべき個人の身体的特徴情報を取得し、当該身体的特徴情報（認証確認データ）と、登録されている登録認証データとを照合することで、本人であるか否かの認証確認を行う。

【０００４】ここで、前記登録認証データとして、個人の身体的特徴の原情報をそのまま登録して利用した場合には、当該登録認証データが盗まれたときに、その悪用を阻止することが困難となる。

【０００５】このため、データの盗難に対処するため、本人の原情報又は原情報から取り出した身体的特徴を、暗号化して前記登録認証データとして登録する方法が採用されている。

【０００６】

【発明が解決しようとする課題】しかしながら、身体的特徴情報に暗号化を施して登録しておいても、暗号化した登録認証データと共に鍵が盗用された場合には復号が可能である。したがって、その鍵の漏洩や紛失などが無いように安全に保管したり、定期的に、鍵の変更処理を施してセキュリティを確保する必要があるなど、鍵の保管・管理業務に大きな手間が掛かるという問題がある。

【０００７】本発明は、このような問題点に着目してなされたもので、暗号化操作や鍵の保管・管理業務が不要であるにも関わらず、登録認証データの盗難による不正な認証の危険性を極力抑えることができる個人認証、つまり、高い安全性及び利便性を有する個人認証方法及びその装置とサーバと端末を提供することを課題とするものである。

【０００８】

【課題を解決するための手段】上記課題を解決するために、本発明は身体的特徴量を用いて本人の認証を行う個人認証方法において、個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成し、該量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成し、該一方向性関数値データと本人確認のために予め用意された登録認証データとを照合し、該一方向性関数値データと登録認証データとが一致した場合には該登録認証データに対応する本人であると判定し、該一方向性関数値データと該登録認証データとが不一致の場合には、前記身体的特徴量と量子化特徴コード列のいずれかに摂動を行い新たな一方向性関数値データを生成すること及びこの生成された一方向性関数値データと前記登録認証データとを照合することとを繰り返し、照合により、該一方向性関数値データと登録認証データとが一致した場合には該登録認証データに対応する本人であると判定し、一致しない場合、前記摂動と照合とを繰り返して当該照合回数が所定回数に達した場合には該登録認証データに対応する本人ではないと判定することを特徴とするものである。

6

【０００９】ここで、量子化とは、特徴量空間を分割し、各区間に量子化値を割りあてることによって、特徴量から量子化値に写像することをいい、摂動とは、対象とする特徴量若しくは特徴コードの値を変動させることをいう。

【００１０】なお、本願発明でいう一方向性関数とは、関数の出力を手掛かりに総当たり以外に入力を特定することが困難である関数のことをさす。例としては、文献 Bruce Schneier, "Applied Cryptography, Second Edition", John Wiley & Sons, Inc., 1996にある、MD5, SHA-1などに記載される一方向性ハッシュ関数、または、それらの関数を複数回組み合わせたものが挙げられる。

【００１１】また、身体的特徴とは、指紋や、音声などがあり、筆跡も身体的特徴の一つである（たとえば、Anil Jain他, "Biometrics－ Personal Identification inNetworked Society －", Kluwer Academic Publishers, 1999を参照）。

【００１２】特徴量を量子化特徴コードに変換したものに一方向性関数を施して得られる一方向性関数値データを登録認証データとして保管するので、該登録認証データが盗難されたとしても、登録されている登録認証データに合致するような身体的特徴情報を生成することは極めて困難となる。よって、安全性が高く、さらに、鍵の保管・管理の手間も不要となり、安全性と共に利便性も向上する。

【００１３】しかし、バイオメトリクス情報は、本人であっても毎回変動する。一方向性ハッシュ関数は、入力の近さと出力の近さが無関係であるため、入力情報と登録情報の類似度を求めることが不可能であり、完全に一致するかどうかによってしか本人性を判断できない。そのため、ある程度の許容度を認める仕組みが不可欠となる。

【００１４】本発明では、特徴量の量子化機構、及び特徴量又は量子化特徴コードへの摂動機構を入れることにより、認証率が高く、かつ安全性も高いシステムを構築

することが出来る。その理由を説明する。

【００１５】まず、量子化の機構のみがある場合を考える。量子化の幅を広くすれば本人拒否率（本人であるのに認証されない割合）が下がり、他人受理率が上がる。また、幅を狭くすれば本人拒否率が上がり、他人受理率（他人であるのに認証されてしまう割合）が下がるというトレードオフの関係がある。よって、適切な幅に設定することによって、所望する本人拒否率、他人受理率を得ることが出来る。

【００１６】しかし、登録情報を盗んで不正に認証を成功させようとする攻撃者においては、各特徴量の量子化された値を推測し、総当たり的に認証に成功する量子化特徴コード列を探索するという攻撃を行うことが考えられる。量子化の幅は狭い方が推測した特徴量列と正解の特徴量列との差分を探索するのに必要な回数が増えるため、攻撃からの安全性は高くなる。

【００１７】そこで、本人認証の際にも、量子化の機構に加えて摂動の機構も入れることによって、それが無い場合よりもより広い範囲の入力を認証することが出来るため、同じ本人拒否率、他人拒否率を保ちつつも量子化の幅を狭くすることが出来ることになる。つまり、より高安全性、高認証率が得られることになる。

【００１８】次に、本発明は与えられた最大認証時間（認証にかかって良い計算時間の上限値）に基づいて、照合を行う最大回数を設定することを特徴とするものである。

【００１９】本発明によれば、認証を行うマシンにおいて、与えられた最大認証時間で行うことの出来る照合回数を最大照合回数と設定することにより、定められた認証時間内で本人認証を行うことが出来る。

【００２０】次に、本発明は、上記量子化操作をする際に使用する、各特徴量空間の分割の方法を記述した量子化パラメータを、各特徴量の分布と、与えられた最高本人拒否率と最大照合回数に基づいて決定するものである。

【００２１】量子化の幅は、認証率、安全性に影響してくる。本発明によれば、与えられた最高本人拒否率（許容される本人拒否率）と最大照合回数に基づいて量子化パラメータを設定することにより、適切な認証率、安全性を持った認証システムを構築することができる。

【００２２】次に、本発明は、上記量子化操作をする際に使用する各特徴量空間の分割の方法を記述した量子化パラメータに、実際には使用しない擬似（ダミー）パラメータを含有させることを特徴とするものである。

【００２３】本発明によれば、実際に使用される特徴量の数を隠すことができ、安全性を高めることができる。

【００２４】次に、本発明は、本人であると判定された際に、取得した身体的特徴の特徴量を加味して新たな特徴量の分布を求め、その新たな特徴量の分布に基づき、量子化する際のパラメータを更新すると共に、当該新たなパラメータに基づき登録されている登録認証データの更新を行うことを特徴とするものである。

【００２５】本発明によれば、より近似精度の高い特徴量分布に基づいて量子化パラメータ及び登録認証データの設定を図ることができ、経時変化にも強い認証が可能となる。

【００２６】次に、本発明は、上記身体的特徴として、筆跡における各ストロークの筆記時間を用いることを特徴とするものである。

【００２７】次に、本発明は、あらかじめ決められた複数の基本ストロークを基準として、上記筆跡における各ストロークに最も類似する上記基本ストロークのストローク番号を、量子化特徴コードとして使用することを特徴とするものである。

【００２８】次に、本発明は、複数の筆跡情報のストローク数の変動を吸収してから登録に用いることを特徴とするものである。

【００２９】次に、本発明は、本人であると認証された場合に得られた、登録認証データに対応する量子化特徴コード列は一定であることを利用して、その量子化特徴コード列を使って個人鍵を生成するものである。本発明によれば、身体的特徴情報ををを入力することにより、本人しか生成することのできない個人鍵を生成することができる。

【００３０】次に、本発明は、身体的特徴量を用いて本人の認証を行う個人認証装置において、個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成する特徴量子化手段と、該量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成する一方向性関数値化手段と、該一方向性関数値データと本人確認のために予め用意された登録認証データとを照合する照合手段と、該一方向性関数値データと該登録認証データとが不一致の場合には、前記身体的特徴量及び量子化特徴コード列のいずれかに摂動を行い新たな一方向性関数値データを生成すること及びこの生成された一方向性関数値データと前記登録認証データとを照合することとを繰り返す探索手段と、前記探索手段において、当該照合回数が所定回数に達しても一致しなかった場合には該登録認証データに対応する本人ではないと判定して認証処理を終了をする認証棄却手段とを有することを特徴とする個人認証装置を提供するものである。

【００３１】次に、本発明は、上記量子化操作をする際に使用する、各特徴量空間の分割の方法を記述した量子化パラメータを、各特徴量に基づいて決定することを特徴とするものである。

【００３２】次に、本発明は、与えられた最大認証時間に基づいて、照合を行う最大回数を設定することを特徴とするものである。

【００３３】次に、本発明は、上記量子化操作をする際

に使用する、各特徴量空間の分割の方法を記述した量子化パラメータを、各特徴量の分布と、与えられた最高本人拒否率と最大照合回数に基づいて決定するものである。

【００３４】次に本発明は、上記量子化パラメータに擬似（ダミー）のパラメータを含ませることを特徴とするものである。

【００３５】次に、本発明は、上記照合手段において一方向性関数値データと登録認証データとが一致した場合に作動して、取得した身体的特徴の特徴量を加味して特徴量の分布を更新し、当該更新後の特徴量の分布に基づき、量子化する際のパラメータを更新する量子化パラメータ更新手段と、量子化する際のパラメータを更新したときに、新たなパラメータに基づき登録されている登録認証データの更新を行う登録認証データ更新手段とを備えることを特徴とするものである。

【００３６】次に、本発明は、上記身体的特徴として、筆跡における各ストロークの筆記時間を用いることを特徴とするものである。

【００３７】次に、本発明は、あらかじめ決められた複数の基本ストロークを基準として、上記筆跡における各ストローク中から最も類似する１又は２以上の上記基本ストロークを、量子化特徴コードとして使用することを特徴とするものである。

【００３８】次に、本発明は、身体的特徴量を用いて本人の認証を行う個人認証のための個人認証サーバにおいて、本人確認のために予め用意された登録認証データを格納する登録認証データ格納手段と、個人の少なくとも１種類の身体的特徴量を量子化して得られる量子化特徴コード列から一方向性関数を用いて一方向性関数値データを生成する一方向性関数値化手段と、該一方向性関数値データと前記登録認証データ格納部に格納される登録認証データとを照合する照合手段とを有することを特徴とする。

【００３９】次に、本発明は、身体的特徴量を用いて本人の認証を行う個人認証のための個人認証端末において、個人の少なくとも１種類の身体的特徴量をそれぞれ量子化して量子化特徴コード列を生成する特徴量子化手段と、該特徴量子化手段で生成された量子化特徴コードを送信する送信手段とを有することを特徴とする。

【００４０】

【発明の実施の形態】次に、本発明の実施形態について図面を参照しながら説明する。

【００４１】図１は、本発明に係る実施形態である個人認証装置の構成を示すブロック構成図であって、身体的特徴情報入力部１、特徴量子化部３、量子化パラメータ格納部５、照合部７、量子化パラメータ更新部９、登録認証データ格納部１１、登録認証データ更新部１３、及び認証結果格納部１５から構成される。

【００４２】まずはじめに、本認証方式の代表的な実施例における登録と認証の処理の流れをそれぞれ図１１を図１２を参照して説明する。

【００４３】登録処理は、図１における身体的特徴情報入力部１から、複数回の身体的特徴情報を採取し（ステップＳ１０１）、各身体的特徴情報について、特徴量子化部３で、正規化、特徴抽出を行って特徴量を得る（ステップＳ１０２）。そこで、各特徴について、特徴量の分布を求め、それにより量子化パラメータを決め、量子化パラメータ格納部５に格納する（ステップＳ１０３）。次に、各特徴の代表値と思われる特徴量（平均値等）を、先ほど設定した量子化パラメータを用いて量子化する（ステップＳ１０４）。

【００４４】次に、量子化によって得られた量子化特徴コードの列を照合部７にある、一方向性関数値化回路７１に送り（ステップＳ１０５）、得られた一方向性関数値データを登録認証データ格納部１１に格納する（ステップＳ１０６）ことによって行われる。

【００４５】認証処理は、身体的特徴情報入力部１から、身体的特徴情報を採取し（ステップＳ２０１）、特徴量子化部３で、正規化、特徴抽出を行って特徴量を得る（ステップＳ２０２）。次に、得られた特徴量を量子化パラメータを用いて量子化する（ステップＳ２０３）。次に、量子化によって得られた量子化特徴コードの列を照合部７に送り、一方向性関数値化回路７１がそれを一方向性関数値に変換する（ステップＳ２０４）。

【００４６】次に比較回路７３が、それを登録認証データ格納部１１にある登録認証データと比較し、一致したかどうかを判定回路７５に送る（ステップＳ２０５）。そこで、一致ならば、認証が成功したとして終了し、一致しなかった場合は、量子化特徴コード列の摂動を行うのであるが、ここで、摂動が今までに何回行われたかをカウントしており、所定の回数を越えた場合は、認証失敗として終了し（ステップＳ２０６）、そうでない場合は探索回路７７に、量子化特徴コード列の摂動を行うように要求する（ステップＳ２０７）。それによって摂動された量子化特徴コード列は再度、一方向性関数値化回路７１に送られて、上記動作を繰り返すことになる。

【００４７】次に、図１を参照して各構成要素の詳説を行い、実施例を説明していく。

【００４８】身体的特徴情報入力部１は、利用者が、例えばタブレットやカメラなどを使用して入力した身体的特徴情報を取得し、当該身体的特徴情報を特徴量子化部３に送る。

【００４９】特徴量子化部３は、入力した身体的特徴情報から身体的特徴を正規化し抽出した後、その身体的特徴に関する複数の特徴量の集合について、各特徴量を量子化パラメータ格納部３にある量子化パラメータを使って量子化して、量子化特徴コードの列Mに変換し、その量子化特徴コードの列Mを照合部７に送る。量子化パラメータ格納部５にある量子化パラメータは、登録時等に

何度か利用者から身体的特徴情報を取得することによって得られた個人の特徴の統計情報に基づいて設定しても良いし、不特定多数の人々から集めた統計情報を使う等の方法により、予め設定しておいてもよい。但し、そのパラメータ情報は記録媒体に保存されるため、その情報から、認証を成功させる量子化パラメータが推測できないような物にしないといけない。その例としては、後に挙げるように各特徴量空間を均等に分割する幅と、その区間の原点からのずれを表すオフセットをパラメータとする例が挙げられる。

【００５０】上記特徴量子化部３の処理について、図２を参照して詳説する。特徴量子化部３は、特徴抽出回路３１、量子化パラメータ設定回路３３、及び量子化回路３５から構成される。

【００５１】ここで、上記身体的特徴情報入力部１及び特徴抽出回路３１が特徴取得手段を構成し、量子化回路３５が特徴量子化手段を構成する。また、量子化パラメータ設定回路３３は、量子化パラメータ設定手段を構成する。なお、本実施形態では、特徴量子化部３は登録処理手段を兼ねる。

【００５２】特徴抽出回路３１は、入力した身体的特徴情報を正規化した後に当該身体的特徴情報から複数の身体的特徴f_i（$i=1, 2, \cdots, n$；nは特徴数）を抽出し、当該各身体的特徴f_iの特徴量q_iを順次、量子化回路３５に送る。

【００５３】但し、量子化パラメータを利用者の特徴の統計情報から設定する場合には、登録モード時に、複数回入力された身体的特徴情報のそれぞれについて上記身体的特徴f_iの各特徴量q_iを量子化パラメータ設定回路３３にも送る。量子化パラメータ設定回路３３は、各特徴について当該複数個の特徴量から特徴量分布を求め当該特徴量の分布に基づき各特徴量毎の量子化パラメータを決定し、その量子化パラメータを量子化パラメータ格納部５に格納する。なお、具体的な量子化パラメータの設定方法については後述する。量子化パラメータ設定回路３３は、登録モードのときにのみ作動する。

【００５４】量子化回路３５は、量子化パラメータ格納部５から、量子化パラメータである量子化する区間の幅w_i及びその区間の原点からのずれを表すオフセットo_iを順次読み出しながら、入力した身体的特徴f_iに対応する特徴量q_iを、図３に表した様に、それぞれ下記の式（１）に従って計算した量子化特徴コードs_i（区間番号）に量子化する。

【００５５】

$$s_i = [q_i / w_i + o_i] \qquad (1)$$

式（１）中、[ ]はガウス記号であり、[ ]内の値を超えない整数値を表わす。

【００５６】量子化回路３５は、上記のような量子化処理を、全ての身体的特徴f_i（$i=1, 2, \cdots, n$）に対応する全特徴量q_iについて施すことで、身体的特徴の列（$f_1, f_2, \cdots, f_n$）に対応する量子化特徴コードの列M（$s_1, s_2, \cdots, s_n$）を求め、当該量子化特徴コードの列Mを照合部７に送る。

【００５７】図４は、身体的特徴f_iについて行う量子化操作の一例であって、各身体的特徴f_1，f_2，…はそれぞれ量子化パラメータである区間幅w_1，w_2，…及びオフセットo_1，o_2，…を使用して量子化される（図４ではオフセットo_iは省略）。身体的特徴f_1，f_2，…の特徴量が●で示すq_1，q_2，…であったとすると、区間番号s_1，s_2，…は、それぞれ２，７，４…となる。

【００５８】図５は行方向に身体的特徴f_iを列方向に量子化後の各区間番号s_iを配置した量子化特徴コード行列であって、○は各特徴に対応する量子化特徴コードを表わしている。矢印で表わされた曲線は、この特徴が個人固有の標準特徴であった場合、量子化特徴コード行列における正解経路を意味している。

【００５９】上記複数回求めた特徴量q_iに基づく量子化パラメータw_i，o_iの設定法としては、例えば次の方法がある。同一の身体的特徴に対する複数の特徴量q_iの頻度分布を平均値m_i、分散σ_i^2の正規分布で近似して分布の大部分を含むように特徴量q_iの変動幅を求め、当該変動幅を少数の区間で含むように上記量子化パラメータw_i，o_iを決定する。例えば、平均値m_iが区間r_i中央に位置し、かつ、区間番号の区間［r_i-1，r_i+1］で特徴量の分布の区間［$m_i-3\sigma_i$，$m_i+3\sigma_i$］を含むことができるように、上記区間の幅w_i及びオフセットo_iを定める。この方法では、特徴量の変動幅、つまり特徴量の変動の大部分を、区間番号r_i-1、r_i，r_i+1の３区間でカバーできる。もっとも、この例のように３区間に拘泥するものではない。

【００６０】また、上記の量子化パラメータを求める例では、特徴量の分布から決定した量子化パラメータw_i，o_iを登録時に求めた固定値とする方法であるが、後述の照合部７において取得した身体的情報が本人のものであると認証された場合に、そのときの特徴量の情報を追加しながら上記特徴量の分布を逐次修正することにより、使用する毎に量子化パラメータw_i，o_iを更新して当該量子化パラメータを逐次更新する量子化パラメータ更新部９を設けても良い。

【００６１】量子化パラメータ更新部９による逐次修正の方法としては、次のような方法が例示できる。すなわち、現在設定されている量子化パラメータw_i，o_iのもとで、照合部７での認証が成功した際に、その成功した量子化特徴コードの列M（区間番号s_iの列）に基づき、下記の（２）式及び（３）式によって、現在の量子化パラメータを設定する基準となっているw_i，o_iを求めることができる。

【００６２】

【数１】

$$m_i = \left(s_i + \frac{1}{2} - o_i\right) w_i \qquad (2)$$

$$\sigma_i = \frac{3}{6} w_i = \frac{1}{2} w_i \qquad (3)$$

このとき、特徴f_iに対応する、k回目に得られた特徴量を$q_{i,k}$、特徴f_i対応する、u個の特徴量から得られた平均を$m_{i,u}$、特徴f_iに対応する、u個の特徴量＊10＊から得られた分散を$\sigma^2_{i,u}$と記述すると、

【数２】

$$m_{i,u} = \frac{\sum_{k=1}^{u} q_{i,k}}{u} \qquad (4)$$

$$\sigma^2_{i,u} = \frac{\sum_{k=1}^{u} (q_{i,k} - m_{i,u})^2}{u} = \frac{\sum_{k=1}^{u} q^2_{i,k}}{u} - m^2_{i,u} \qquad (5)$$

であるため、$m_{i,u+1}$, $\sigma^2_{i,u+1}$は、

【数３】

$$m_{i,u+1} = \frac{\sum_{k=1}^{u+1} q_{i,k}}{u+1} = \frac{\sum_{k=1}^{u} q_{i,k} + q_{i,u+1}}{u+1} = \frac{u \cdot m_{i,u} + q_{i,u+1}}{u+1} \qquad (6)$$

$$\sigma^2_{i,u+1} = \frac{\sum_{k=1}^{u+1} (q_{i,k} - m_{i,u+1})^2}{u+1} = \frac{\sum_{k=1}^{u+1} q^2_{i,k}}{u+1} - m^2_{i,u+1} = \frac{\sum_{k=1}^{u} q^2_{i,k} + q^2_{i,u+1}}{u+1} - m^2_{i,u+1} = \frac{u \cdot (\sigma^2_{i,u} + m^2_{i,u}) + q^2_{i,u+1}}{u+1} - m^2_{i,u+1} \qquad (7)$$

である。

【００６３】従って、既知のm_i, σ_iが例えば過去１００回のデータから求められた値とする。つまり、$m_i = m_{i,100}$, $\sigma_i = \sigma_{i,100}$とすると、逐次修正された後の平均値及び分散$m_i' = m_{i,101}$, $\sigma' = \sigma_{i,101}$は、今回得られた特徴量$q_{i,101}$と既知の$m_{i,100}$, $\sigma_{i,100}$から、上記の（６）式及び（７）式を使って求めることができる。このように、上記逐次修正によって特徴量の分布の近似の精度を向上させることができる。

15

【００６４】そして、量子化パラメータ更新部９が、新たに得られた$m_{i,}$、$\sigma_{i,}$から上記の量子化パラメータ設定方法に基づいて、新たに逐次修正された量子化パラメータ$m_{i,}$、$\sigma_{i,}$を求め、その量子化パラメータ$m_{i,}$、$\sigma_{i,}$に量子化パラメータ格納部５の量子化パラメータを更新する。また、量子化パラメータを更新したときは、登録認証データ更新部１３によって、逐次修正された量子化パラメータに基づき、新たな登録認証データを求めて登録認証データ格納部１１に格納されている登録認証データを更新しておく。

【００６５】新たな登録認証データを求める方法の例としては、入力される特徴量として更新後の各特徴量の平均値$m_{i,}$、$\sigma_{i,}$を使い、それと更新された量子化パラメータにより登録を行う方法が挙げられる。

【００６６】次に、照合部７は、特徴量子化部３から入力した量子化特徴コードの列Mに一方向性関数を施すことによって一方向性関数値データを求め該一方向性関数値データを認証確認データとして、当該認証確認データと登録認証データ格納部１１に登録してある特定個人の登録認証データ（一方向性関数値データ）とを比較・照合して、本人であるか否かの認証情報を認証結果格納部１５に蓄積する。また、上記照合が不一致の場合には、上記量子化特徴コードに摂動を加えて当該量子化特徴コードを更新しながら、所定回数だけ上記照合操作を繰り返し、所定回数の照合操作を行っても不一致の場合は、本人のものではないと判定し棄却する。

【００６７】上記照合部７の処理を、図６を参照して詳説する。照合部７は、図６に示す構成図のように、一方向性関数値化回路７１、比較回路７３、判定回路７５、及び探索回路７７からなる。

【００６８】ここで、一方向性関数値化回路７１が一方向性関数値化手段を構成し、比較回路７３及び判定回路７５が照合手段を構成し、探索回路７７が探索手段及び認証棄却手段を構成する。なお、本実施形態では、一方向性関数値化回路７１が登録処理手段を兼ねる。

【００６９】一方向性関数値化回路７１は、入力した量子化特徴コードの列Mを、一方向性関数によって一方向性関数値データH（M）に変換し、その一方向性関数値データH（M）を認証確認データとして比較回路７３に送る。

【００７０】その例としては、一方向性関数Hとして、ビット列を入力とするＳＨＡ－１を用い、各量子化値を３２ビットとし、上記入力する量子化特徴コードの列M＝s_1，s_2，s_3，…，s_nを、

$s_1 \times 2^{32\times 0} + s_2 \times 2^{32\times 1} + \cdots + s_n \times 2^{32\times (n-1)}$

のビット列によって表現し、それを入力として一方向性関数に入力する方法が挙げられる。

【００７１】登録モードの場合には、一方向性関数値化回路７１は、求めた一方向性関数値データを登録認証データH（M_r）として登録認証データ格納部１１に格納する。

16

【００７２】比較回路７３は、登録認証データ格納部１１に格納されている登録認証データH（M_r）を読み出し、認証確認データH（M_c）と比較する。

【００７３】判定回路７５は、比較回路７３での比較結果が「一致」であれば、入力された身体的特徴情報が登録認証データ格納部１１に登録された本人のものであると判定し、その結果を認証結果格納部１５に送る。また、「不一致」であれば、再度認証を行うために探索回路７７に起動をかける。

【００７４】但し、比較回路７３は探索回路７７自体の起動回数をカウントしていて、当該カウントが所定値以上になった場合には、上記探索回路７７の起動を行うことなく、入力変動が想定外に大きかったか、あるいは、他人の身体的特徴情報が入力されたものとみなして、認証棄却情報を認証結果格納部１５に送り、照合部７の処理を終了する。

【００７５】探索回路７７は、特徴量子化部３から入力した量子化特徴コードの列Mの値に対し、所定規則によって決められた方法による摂動を加えることで、新たな量子化特徴コードの列M’を求め、その新たな量子化特徴コードの列M’を一方向性関数値化回路７１に送る。これによって、再度の比較・照合操作が行われる。

【００７６】上記摂動は、対象とする特徴コードの変動幅内で当該特徴コードの値を変更する。本実施形態の例では、量子化パラメータ設定回路３３において、各特徴量について、３つの区間で上記変動幅を含むことができるように各特徴量に対応する量子化パラメータの区間の幅を決定しているので、対象とする特徴コードについて±１の変動量の範囲で摂動を行う。

【００７７】次に、その摂動の方法の一例を説明する。

【００７８】まず、身体的特徴f_iに対応する特徴コード（区間番号）s_1に±１の摂動を加えることにより新たな量子化特徴コードの列M’＝s_1＋１，s_2，s_3，…，s_nを生成する。これを、起動されるたびに、上記操作をs_2，s_3，…，s_nで繰り返す。この操作は入力の身体的特徴情報から得られたｓｉの経路からｓ，ｉ＝１，２，３，…，ｎの順にずらしながら図５で述べた正解経路を探索していることに相当する。

【００７９】図７は経路探索の一例を示す図であり、破線は入力の量子化特徴コードの列M_cの経路を、矢印はs_1＝１からs_1＝２への＋１の摂動をそれぞれ表している。図７ではM_cの経路は図５の正解経路と一致していないが、摂動を加え経路の変化させることにより正解経路を探し得ていることがわかる。

【００８０】さらに、各量子化特徴コードs_1，s_2，s_3，…，s_nの全てに＋１の摂動を加えても、不一致であった場合には、今度はs_1に対し、－１の摂動を加えることにより生成された新たな量子化特徴コードの列

$M'' = s_1 - 1, s_2, s_3, \cdots, s_n$ を作成して出力する。この操作を、起動されるたびに、$s_2, s_3, \cdots, s_n$ について順次まで－１の摂動を繰り返す。さらに、起動が掛けられた場合、つまり不一致の場合には、±１の範囲で、任意の２つのs_i, s_j（$i<j$）の組み合わせについて摂動を行う。さらに、起動が掛けられた場合、つまり不一致の場合には、任意の３つ、それでも起動された場合は４つ、５つ、…ｎ個と試していく。

【００８１】上記摂動方法の説明では、±１の範囲での任意のｎ個についての摂動までを行う方法を示したが、その回数まで探索回路７７を起動する必要はなく、あらかじめ決められた摂動回数に達した時点で、認証処理を終了して棄却情報を認証結果格納部１５に供給しても良い。また、特徴によっては、他の摂動の順番の方が、少ない回数で一致が発見される確率が高ければ、摂動の順番は変えてもよい。

【００８２】また、上記の摂動の例では、摂動をs_iに加える方法を示したが、特徴によっては、特徴の頻度分布を考慮して、摂動を特徴量q_iに加える方法であってもよい。但しこの場合には、上記特徴量子化部の起動が要求される。

【００８３】次に、探索・照合を行う最大回数を、予め定められた最大認証時間（認証にかかって良い計算時間＊＊の上限値）に基づいて設定する方法の一例を示す。

【００８４】例えば、予め定められた最大認証時間をT_{max}とすると、照合を行う計算機上で、数個の身体的特徴情報のサンプルについて認証処理を行い、T_{max}内で行うことのできた照合回数の平均をとるなどというようにして決めることができる。

【００８５】次に、量子化パラメータを、各特徴量の分布と、与えられた最高本人拒否率P_{rej}と最大照合回数T_{max}に基づいて設定する方法の一例を示す。

【００８６】各特徴量q_iの分布を平均値m_i、分散σ_i^2の正規分布と近似して、T_{max}回の摂動で含むことができない分布の範囲が最大本人拒否率P_{rej}の分以下になるように、量子化パラメータw_i，o_iを決定することを考える。

【００８７】摂動しない場合、一回の試行で本人拒否率がP_{rej}以下になる条件を満たすには、各特徴に対して、一量子化区間の幅w_iの標準偏差σ_iに対する割合を一定にする、つまりその割合を２Ｒとして、全てのｉについて$w_i = 2R\sigma_i$とすると、特徴の数をｎとし、区間［$m_i - R\cdot\sigma_i, m_i + R\cdot\sigma_i$］がカバーする分布の割合が、

【数４】

$$(1-P_{rej})^{\frac{1}{n}}$$ になるようなＲを求めれば良い。

そのようなＲは、

$$\Phi(-R) = \frac{1-(1-P_{rej})^{\frac{1}{n}}}{2}$$

を満たせば良いので、

$$R = -\Phi^{-1}\left(\frac{P_{rej}}{2n}\right) \qquad (8)$$

によって求められる。但し、Φ（ｚ）を標準正規分布の分布関数、つまり、

【数５】

$$\Phi(z) = \int_{-\infty}^{z} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx$$

とする。また、P_{rej}を十分０に近いとして近似を行った。

【００８８】これで、各特徴f_iについて、

【数６】

$$2R\sigma_i = -2\Phi^{-1}\left(\frac{P_{rej}}{2n}\right)\sigma_i$$

を基準となる量子化幅とする。

【００８９】これは摂動を考えない場合であったので、摂動を加えることによって、いくつかの量子化幅は狭くすることができる。

【００９０】上記の摂動の様に進めることを考える。

【００９１】Search（$d_0, d_1, d_2, \cdots$）を、合計Ｎ個の特徴量について、シフトしない特徴の数がd_0個、±１シフトする特徴の数がd_1個、±２シフトする特徴の数がd_2個、…である摂動の組合せを全通り探索することを表すとすると、探索は以下の表の上から下に進むこととなる。

【００９２】

【表１】

19

	d_0	d_1	d_2	d_3	…	
Search	(N					*
Search	(N－1	1	)			*
Search	(N－2	2	)			*
…						
Search	(0	N	)			*
Search	(N－1	0	1	)		
Search	(N－2	1	1	)		
…						
Search	(0	N－1	1	)		*
Search	(N－2	0	2	)		
Search	(N－3	1	2	)		
…						
Search	(0	N－2	2	)		*

ここで、例えばSearch（N－１，１）まで探索が可能であったとすると、一つの特徴を±１シフトする組合せを全通り試すことができるので、任意の一つの特徴について、その量子化幅を１／３に狭めても目的の本人拒否率を達成できることを意味する。

【００９３】上記の探索において、＊印がついている所に達する毎に、量子化幅をより狭めることができる。

【００９４】よって、T_{max} 回の摂動によって、どこの＊印まで達成できるかを計算できれば、どれだけ量子化幅を狭めることができるかを決定することができる。

【００９５】＊印のついたところをまとめると以下のような表になる。

【００９６】

【表２】

d_0	d_1	d_2	d_3	…
N				
N－1	1			
N－2	2			
…				
0	N			
0	N－1	1		
0	N－2	2		
…				
0	0	N		
0	0	N－1	1	
…				
0	0	0	N	

W_e（N）を、Search（０，０，…，N（＝d_e））にたどり着いて探索し終るまでの総試行回数とし、PW_e（i，N）をSearch（d_0，d_1，…，d_{e-1}，i（＝d_e））についてすべてのd_0，d_1，…，d_{e-1}を尽くす試行回数とすると、

$$W_e(N) = (2e+1)^N \quad (1)$$

$$PW_e(i,N) = {}_N C_i \cdot 2^i \cdot W_{e-1}(N-i) \quad (2)$$

と表すことができる。

【００９７】よって、下の手順を行うことによってどこまで到達できるかが分かる。

【００９８】１．W_{e-1}（N）≦T_{max}＜W_e（N）となるｅを求める

２．r：＝T_{max}－W_{e-1}（N）

３．for(i:=1; r≧0;i:=i+1){r:=r-PW_e（i,N)}

４．i：＝i－２

５．if(i==0){e：＝e－１；i＝N}

到達点は、Search（０，０，…，N－i，i（＝d_e））となる。

【００９９】よって、任意のｉ個の特徴について、量子化幅を基準の幅の１／（２ｅ＋１）にすることができ、任意のN－ｉ個の特徴について、量子化幅を基準の幅の１／（２ｅ－１）にすることができる。

【０１００】以上の方法によって、量子化パラメータを、各特徴量の分布と、与えられた最高本人拒否率と最大照合回数に基づいて設定することができる。

【０１０１】次に、認証を成功させた摂動後の量子化特徴コードを使って個人鍵を作成する方法について述べる。図１０は、個人鍵を生成し得る個人認証装置の構成を示すブロック図である。

【０１０２】図１０に示す個人認証装置は鍵の生成機能を有するもので、図１に挙げた個人認証装置の基本構成と身体的特徴情報入力部１、特徴量子化部３、量子化パラメータ格納部５、照合部７、量子化パラメータ更新部９、登録認証データ格納部１１、登録認証データ更新部１３の部分で略同一であるが、照合部７に鍵生成部１７が接続されている点が異なる。またこれにより照合部７は、認証が成功した場合には、その認証を成功させた摂動後の量子化特徴コード列を鍵生成部１７に送るという構成になっている。

【０１０３】鍵の生成方法としては、以下のような方法が考えられる。

【０１０４】例えば、一方向性関数H_1として、任意長のビット列を入力として固定長の出力を生成する既知の一方向性関数ＳＨＡ－１を用い、各量子化値を３２ビットとし、上記量子化特徴コードの列M＝s_1，s_2，s_3，…，s_nを、

$$s_1 \times 2^{32\times 0} + s_2 \times 2^{32\times 1} + \cdots + s_n \times 2^{32\times(n-1)}$$

と表し、それと、記録媒体にあらかじめ格納しておいた乱数Ｒを足し合わせた数Ｌをビット列によって表現し、それにH_1を施すことによって、固定長の個人鍵H_1（Ｌ）を生成することが出来る。

【０１０５】また、H_1（Ｌ）を共通鍵暗号の鍵として使うと、複数の鍵K_1，K_2，…、K_vで暗号化したものを記憶媒体に格納しておき、必要な際には再度H_1（Ｌ）を生成して復号化することにより、複数の鍵の生成も行うことが出来る。

【０１０６】この様に、暗号化を使えば、複数の鍵に限らず、秘密にしておきたいデータの保護にも使用することが可能である。

【０１０７】また、他の方法としては、複数の鍵K_1，

K_2，…、K_vが全てH_1（Ｌ）の長さ以下であれば、複雑な暗号化を使わなくても

K_1＃H_1（Ｌ），k_2＃H_1（Ｌ），…K_v＃H_1（Ｌ）

（なお、ここでは「＃」を排他的論理和を示すものとする）を記憶媒体に入れておき、欲しい時にはもう一度排他的論理和をとることによって得ることが出来る。

【０１０８】次に、上記構成の個人認証装置の作用・効果等について説明する。

【０１０９】従来の個人認証法では、例えば指紋を身体的特徴とした場合にはマニューシャ、筆跡を身体的特徴とした場合にはｘ－ｙ座標の筆点座標系列と筆圧等に見られる如く、身体的特徴から身体的特徴情報の原情報の近似的再現を可能とする特徴が多用されていた。また、認証方法としては特徴間の類似度的尺度を用いて判定する場合が多く、入力されて特徴が登録特徴と同一でなくとも類似していれば本人と認証される仕組みとなっていた。したがって、登録特徴が盗難されると、該特徴から登録に用いられた身体的特徴情報が近似的に再現され、個人認証システムの入力として用いられるとセキュリティが破られる恐れがあった。

【０１１０】これに対し、本発明に基づく上記装置においては、特徴そのものを保管せず、量子化して量子化特徴コードに変換したものに、更に一方向性関数を施して得られる一方向性関数値データを登録認証データとして登録し、当該一方向性関数値データ同士で照合する。したがって、登録認証データ格納部１１に格納されている登録認証データが盗難されたとしても逆変換ができないため、登録認証データに合致する身体的特徴情報の再現は極めて困難となる。

【０１１１】また、量子化パラメータw_1，o_1が盗難されたとしても、身体的特徴f_iに対応する量子化特徴コード（区間番号）s_iの最大値をｋ－１とすると、量子化特徴コード行列における経路の組合せはk^n通りある。つまり、量子化パラメータ及び登録認証データを盗み、正解を探索しようとした場合、最大k^n通りの組み合せを調べなくてはいけない。ｋ，ｎが不明な状態では、取り得る経路の組合せは理論上、無限大となり、正解経路を発見するのは極めて困難である。これらのことから、本発明に係る本実施形態では、登録認証データ等の盗難に係わる危険性が極力低減されている。

【０１１２】上記で示したように、不正に正解を探索しようとした場合、ｋ，ｎが大きいほど探索が困難になるため、ｋ，ｎは大きなほうが安全性が高いことになる。つまり、量子化区間幅w_iは小さなほうが安全性が高いわけである。

【０１１３】しかし、小さくしすぎると、身体的特徴量にはばらつきがあるので、本人であっても認証できなくなる可能性がある。そこで、摂動を繰り返して照合を繰り返すことにより、摂動をしない場合よりも量子化区間幅を狭くしつつ、本人拒否率も上げることのない認証が可能となる。つまり、安全性が高く、信頼性も高い認証が可能となる。

【０１１４】また、探索・照合の回数と量子化パラメータの決め方であるが、探索・照合の回数を最大認証時間に基づいて決め、量子化パラメータを個人の特徴量の分布と、予め定められた最高本人拒否率と最大認証時間に基づいて決めることにより、認証率、安全性、認証にかかる処理時間が現実的に使用可能なように調整できる。

【０１１５】上記で示した方法によると、その最高本人拒否率と最大認証時間を満たす条件において、不正に正解を探索する攻撃に対して最も安全になるように摂動回数と量子化パラメータを決めることが可能となる。

【０１１６】さらに、量子化パラメータを逐次変更する場合には、特徴量分布の近似の精度を上げることができるため、より安定した認証が可能となる。

【０１１７】次に、上記ｋ，ｎを不明にできる効果的な実施例として手書き署名の筆跡の各ストロークの筆記時間を身体的特徴量として用いる場合の実施例を図８を用いて説明する。図８は「通研」と署名した例であり、ストローク１～ストローク１６の１６画からなる。いま、身体的特徴f_iとしてｉ番目のストロークの筆記時間をとり特徴量ｑ(msec）で表現する。これが量子化され更に一方向性関数値に変換されて上述の照合処理が行われる。なお、ここでは筆記時間はペンダウンからペンアップまでの筆点からなる実ストロークの時間とし、筆跡から各ストロークに分解するにはペンダウンからペンアップまでの時間をもって代表される。

【０１１８】ここで、各ストロークの筆記時間は、個人内変動の小さい特徴の一つとして選択されたものである。

【０１１９】また、図８の例では、特徴f_iとしてペンダウンからペンアップまでの筆点からなる実ストロークの筆記時間をとったが、ペンアップからペンダウンまでの直線で表される仮想ストロークの筆記時間をも併せて用いてもよい。

【０１２０】ここで、セキュリティを向上させるために、特徴量の数ｎを不明にさせる方法として、量子化パラメータ格納部３が特徴番号ｎ＋１以降の量子化パラメータをダミーで有する方法を例として挙げることができる。これにより、その署名の書かれ方を知っている人以外はｎの真の値を分からなくさせることができる。

【０１２１】擬似パラメータ（ダミーの量子化パラメータ）w_{n+1}，…、o_{n+1}，…の設定方法としては、例えば、w_iの分布を、平均値m_{i+1}、分散σ_{i+1}^2の正規分布で近似し、その分布にしたがった数列をランダムに生成し、それをw_{n+1}以降の値とし、o_{n+1}，…の方は、［０，１）のランダムな値とする方法がある。

【０１２２】また、上記各ストロークに基づく特徴量に加えて、基本ストロークの情報を加えると探索すべき経

路の数を更に飛躍的に増大させることができる。すなわち、特徴抽出回路２１において、入力されたストロークに対して、基本ストロークの中で最も距離の近い１又は２以上の基本ストロークを選択して、そのストローク番号を量子化特徴コードとして使用する。ストローク間の距離の計算法としては、 Toru Wakahara, Hiroshi Murase, Kazumi Odaka, ''On-line Handwriting Recognition'', Proceedings of The IEEE, Vol.80,No.7, July 1992にある方法を使用することが出来る。

【０１２３】例えば、図９に示すR₁，R₂，R₃，R₄，…は基本ストロークの一例であって、入力された各ストロークから、上記基本ストロークの中で最も距離の近いものを選択して、そのストローク番号を量子化コードとして割り当てる。例えば、図８のストローク１はR₃に割り当てられ、ストローク番号である３を量子化特徴コードとする。

【０１２４】ここで、上記各基本ストロークは、多人数の筆記者の多数回筆記により作成された大量データの分析結果に基づき、文字を表現する多数のプリミティブの集合の中から個人性が現れ易いものを選択すること等により得ることができる。

【０１２５】次に、複数の筆跡情報におけるストローク数を等しくする方法の一例を示す。

【０１２６】筆跡情報として、筆圧の時系列データをｋ回採取したとする。そのデータの２つを選び出す全ての組合せに、既知の技術である、dynamic programming(DP)法を適用し、b_0番目のデータが、他のデータとの距離の合計が最小であったときそれを基本データとする。

【０１２７】dynamic programming法については、例えば、文献 Hiroaki Sakoe, Seibi Chiba, "Dynamic Programming Algoritthm Optimization for Spoken Word Recognition",IEEE Trans. on Acoustics, Speech, and Signal Processing, Vol. ASSP-26,No.1,Feb.1978に記載されている。

【０１２８】記法として、m番目のデータのペンのアップ／ダウンの時間を$t_m^{(m)}(1)$，$t_m^{(m)}(2)$，…と表現する。

【０１２９】次に基本データ以外の全てのデータｍ（ｍ≠b_0）について、$t_m^{(b0)}(i)$,に、ＤＰによって写像された時系列空間上で一番近い$t_m^{(m)}(j)$を求め、それを$t_m^{(b0)}(i)$の対応点と考え、$c^{(b0,m)}(i)=j$と表現する。

【０１３０】次に、各データｍについて、データｍの一つのペンアップ／ダウンの時間にデータb_0の複数のペンアップ／ダウンの時間が対応している、つまり、あるｊ´について$c^{(b0,m)}(i_1)=c^{(b0,m)}(i_2)=\cdots j'$となった場合は、$t_m^{(b0)}(i_1)$,$t_m^{(b0)}(i_2)$,…をｍの時間軸上に写像したもので、一番$t_m^{(m)}(j)$に近かった点、$t_m^{(b0)}(i_h)$のみを対応点として認め、それ以外のものについては$c^{(b0,m)}(i_1)=-1$（ｌ≠ｈ）して対応点でないとする。

【０１３１】次に、各$t_m^{(b0)}(i)$において、全てのデータｍ（ｍ≠b_0）について対応点が 存在する、つまり、全てのｍについて$c^{(b0,m)}(i)\neq -1$であったなら、そのｉ について各$t_m^{(1)}(i)$を、画の切れ、つながりによって消滅することの少ない安 定したペンアップ／ダウンの時間$t'_m{}^{(1)}(i')$とする。

【０１３２】安定したペンアップ／ダウンの時間として認められなかった点は全てを取り除き、各データについて得られた$t'_m{}^{(1)}(i')$をペンアップ／ダウンの時間として 考え、各データのストローク時間とする。

【０１３３】また、上記実施形態では、登録認証データの作成及び登録も、特徴量子化部３や照合部７を通じて行っているが、当該登録認証データの作成及び登録の処理を行う処理を別ブロック（別装置）としても良い。

【０１３４】また、本認証を行う装置を、認証を行うサーバと、利用者が身体的特徴情報を入力する端末に分けて使用しても良い。

【０１３５】その例としては、図１における身体的特徴情報入力部１を個人認証端末にして、残りの部分を個人認証サーバとして、身体的特徴情報入力部１と特徴量子化部を繋ぐ部分をネットワークとする方法と、身体的特徴情報入力部１と特徴量子化部３と量子化パラメータ格納部５を個人認証端末にして、残りの部分を個人認証サーバとして、特徴量子化部３と照合部７を繋ぐ部分をネットワークとする方法がある。

【０１３６】認証結果を端末側が知りたい場合は、サーバと端末間に認証結果を送受信する手段をつけることによって可能となる。

【０１３７】また、後者の実現方法において、認証に成功した際の身体的特徴の特徴量を加味して得られた新たな特徴量分布に基づき、量子化パラメータ、登録特徴量データを更新することを行いたい場合は、その更新をする際に必要とされるデータの送受信を行うことの出来る手段をつけることによって可能となる。

【０１３８】ただし、身体的特徴情報、もしくは量子化特徴コードをそのまま送信する場合は、個人認証サーバと個人認証端末を繋ぐネットワーク回線については、盗聴、改ざんの心配のないようなイントラネット等でないといけないことは言うまでもない。

【０１３９】以上において、本発明の実施形態について具体的に説明したが、本発明は上記実施形態に限定されるものではなく、その主旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【０１４０】

【発明の効果】以上説明したように、本発明によれば、身体的特徴情報から得られる特徴の特徴量を量子化操作により量子化特徴コードに変換し、該量子化特徴コードの列に一方向性関数を施して生成される一方向性関数値データを登録認証データとして格納しておき、新たに身

体的特徴情報が入力されると、入力から得られた特徴量、あるいは、量子化特徴コードに適宜、摂動を加えながら、得られた量子化特徴コードを一方向性関数値に変換し登録認証データとの照合を行うので、登録認証データが盗難されたとしても逆変換ができないため、登録されている登録認証データに合致する身体的特徴情報の再現は極めて困難であるため、安全性や信頼性の高い認証方法であると共に、入力された身体的特徴の変動にも対処される。すなわち、毎回変動する身体的特徴に対処して安定した認証を可能にするという効果がある。

【０１４１】また、登録特徴を暗号化して保管しておく従来方式と比べて、鍵の保管・管理の手間も不要となる長所がある。

【０１４２】また、本発明によれば、与えられた最大認証時間に基づいて最大照合回数を求めること、また与えられた最高本人拒否率と最大照合回数に基づいて量子化パラメータを決めることにより、認証率、安全性、認証時間が現実的に使用可能なように調整できる。

【０１４３】例えば、求められる最高本人拒否率と最大認証時間を満たす条件下で安全性が最大になるように量子化幅と摂動回数を決めることが可能になる。

【０１４４】また、本発明によれば、量子化パラメータ中に擬似パラメータを含むことにより特徴量の数が不明となり、認証システムの安全性が向上するという効果がある。

【０１４５】また、本発明によれば、認証が成功したときの身体的特徴の特徴量を用いて、新たな特徴量の分布を求めることにより、より近似精度の高い特徴量分布に基づいて量子化パラメータを設定することができるため、毎回変動し、また経時変化しやすい身体的特徴情報の特徴に対処し安定した認証を行うことができ、より認証の信頼性が向上するという効果がある。

【０１４６】また、本発明によれば、署名の筆跡の各ストロークの筆記時間を身体的特徴量として用いること、又は、最も類似する基本ストロークのストローク番号を量子化特徴コードとして用いることにより、上記実施例で述べた各効果を得ることができる。

【０１４７】また、本発明によれば、身体的特徴量から個人鍵を生成することにより、銀行のＡＴＭにおける暗証番号やシステムのログインの時に必要とされるパスワードなどの本人が秘密を持っておかなくてはいけない記号列等を、本人の記憶にも頼ることなく安全に保管し、生成することが可能である。

【０１４８】また、本発明によれば、個人認証サーバと個人認証端末を用いて認証を行うことにより、身体的特徴を取得する場所と、照合を行う場所を異にすることができるという効果がある。

【０１４９】また、本発明によれば、複数の筆跡情報からストローク情報を抽出する際に、該筆跡情報間のストローク数の変動を吸収し、全データのストローク数を等しくした後に得られた各ストロークの筆記時間を身体的特徴量として用いて登録認証データを作成することにより、ストローク間がつながったり切れたりしやすい筆跡においても、ストローク数が違うことによる登録の失敗を減らすことが出来、安定した登録を可能にする。

【図面の簡単な説明】

【図１】本発明に基づく実施形態に係る個人認証装置のブロック構成図である。

【図２】本発明に基づく実施形態に係る特徴量子化部の構成図である。

【図３】量子化パラメータとして、量子化幅ｗ，とオフセット量子化ｏ，を使った量子化の例を示す図である。

【図４】量子化操作の一例を示す図である。

【図５】量子化特徴コード行列の一例を示す図である。

【図６】本発明に基づく実施形態に係る照合部の構成図である。

【図７】量子化特徴コード行列における量子化区間番号の摂動の一例を示す図である。

【図８】身体的特徴情報として筆跡を用いた場合の一例を示す図である。

【図９】筆跡における基本ストロークの一例を示す図である。

【図１０】個人鍵生成を行う個人認証装置のブロック構成図である。

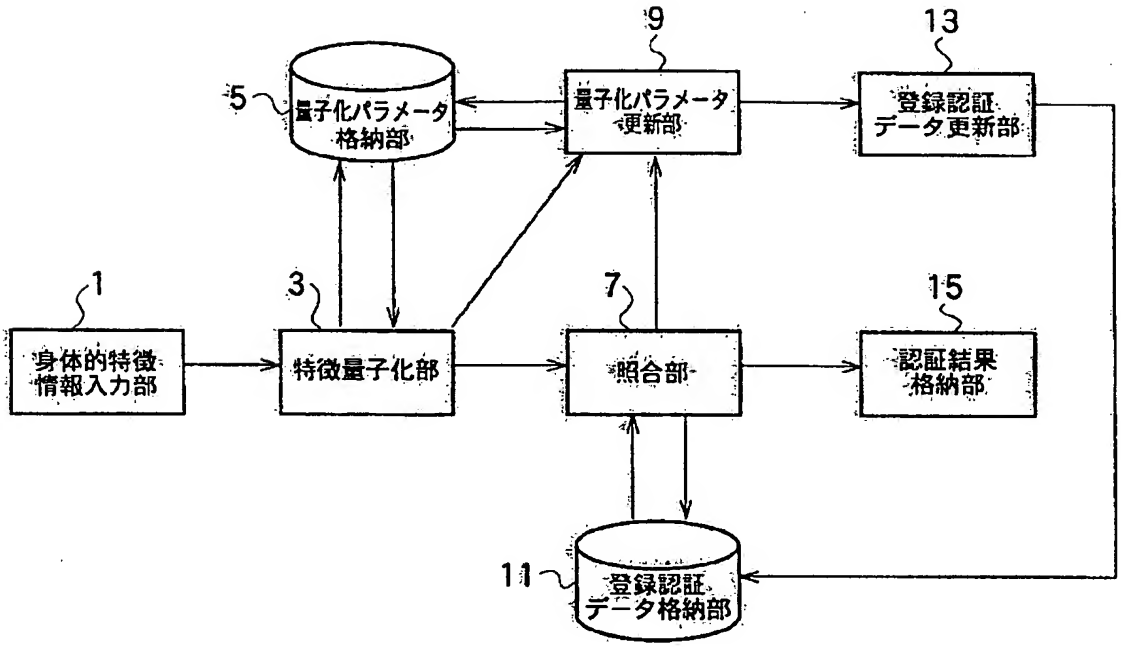
【図１１】登録処理の処理手順の一例を示すフローチャートである。

【図１２】認証処理の処理手順の一例を示すフローチャートである。

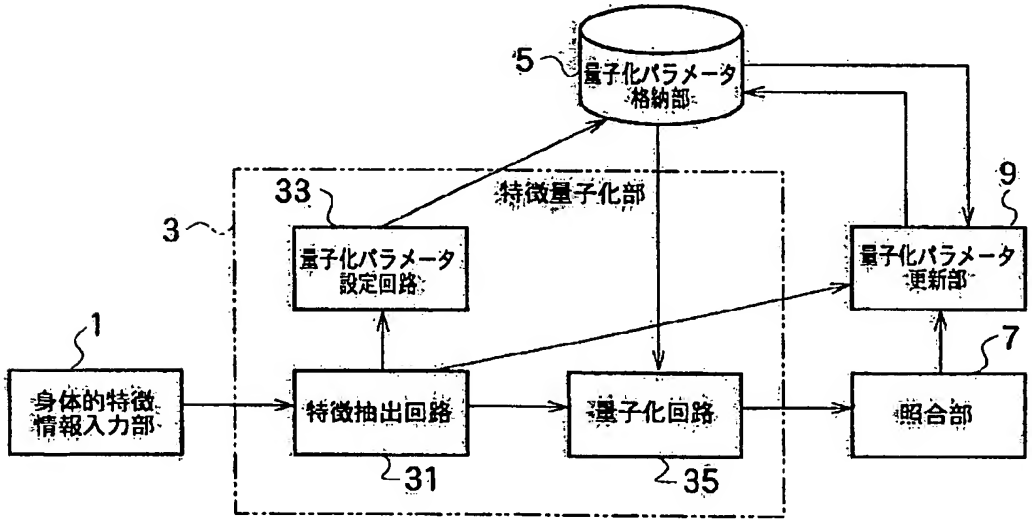
【符号の説明】

１　身体的特徴情報入力部
３　特徴量子化部
５　量子化パラメータ格納部
７　照合部
９　量子化パラメータ更新部
１１　登録認証データ格納部
１３　登録認証データ更新部
１５　認証結果格納部
１７　鍵生成部
３１　特徴抽出回路
３３　量子化パラメータ設定回路
３５　量子化回路
７１　一方向性関数値化回路
７３　比較回路
７５　判定回路
７７　探索回路

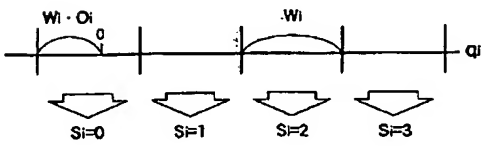
【図１】


9
13
5
量子化パラメータ格納部
量子化パラメータ更新部
登録認証データ更新部
1
3
7
15
身体的特徴情報入力部
特徴量子化部
照合部
認証結果格納部
11
登録認証データ格納部

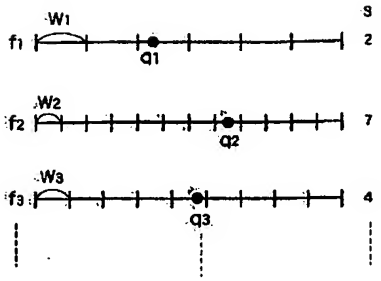
【図２】


5
量子化パラメータ格納部
特徴量子化部
33
3
9
量子化パラメータ設定回路
量子化パラメータ更新部
1
7
身体的特徴情報入力部
特徴抽出回路
量子化回路
照合部
31
35

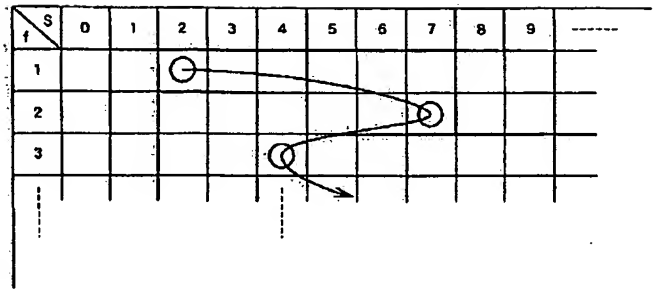
【図３】


Wi・Oi
0
Wi
qi
Si=0
Si=1
Si=2
Si=3

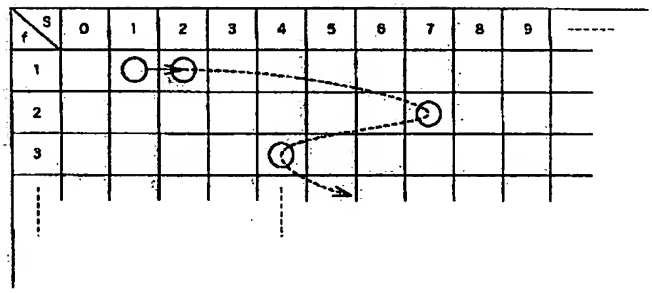
【図４】


W1
f1
q1
S
2
W2
f2
q2
7
W3
f3
q3
4

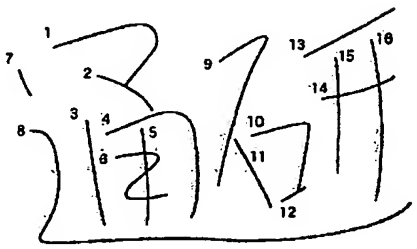
【図５】


S
f
0
1
2
3
4
5
6
7
8
9
1
2
3

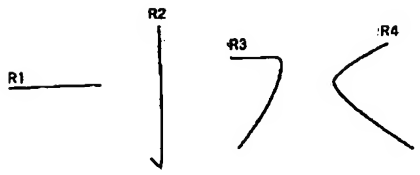
【図７】


S
f
0
1
2
3
4
5
6
7
8
9
1
2
3

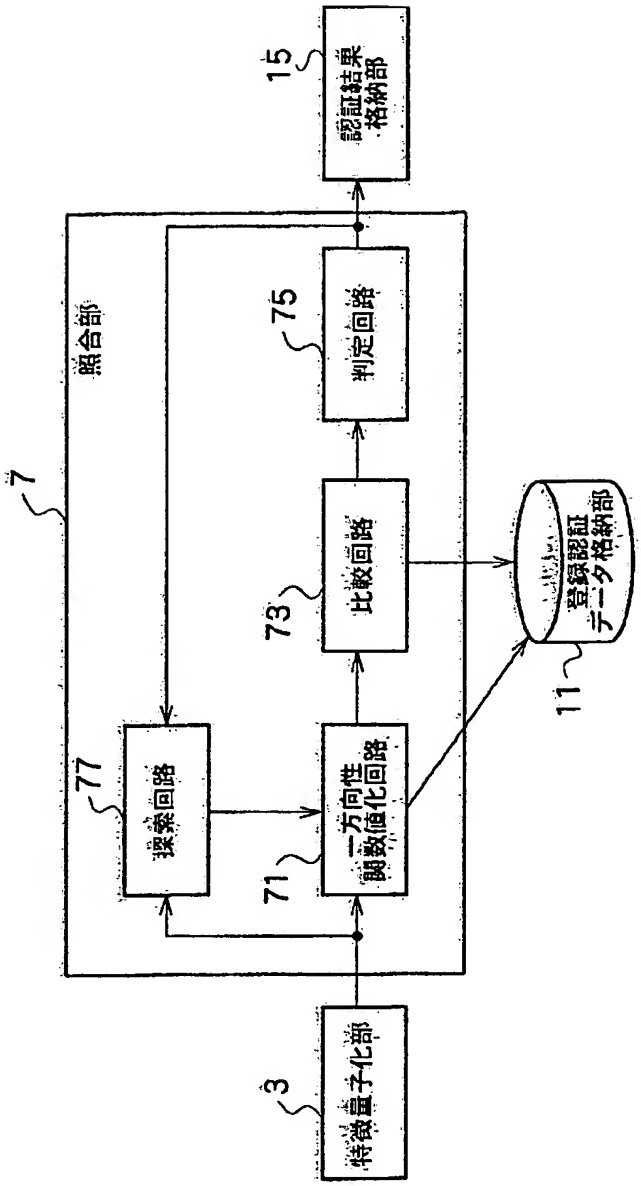
【図８】


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16

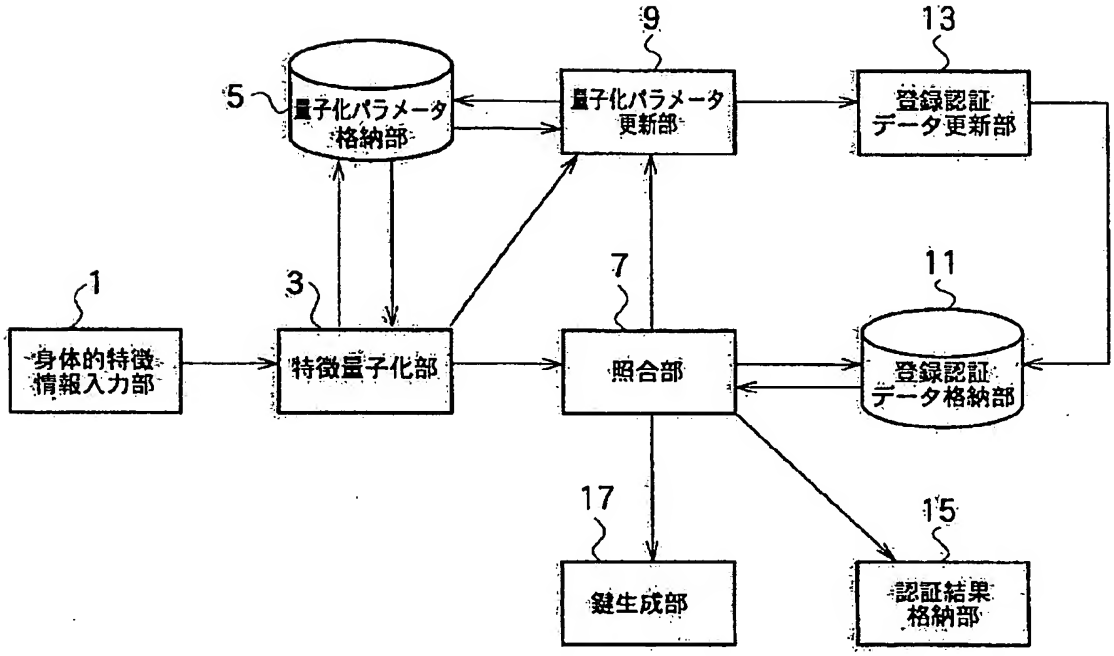
【図９】


R1
R2
R3
R4

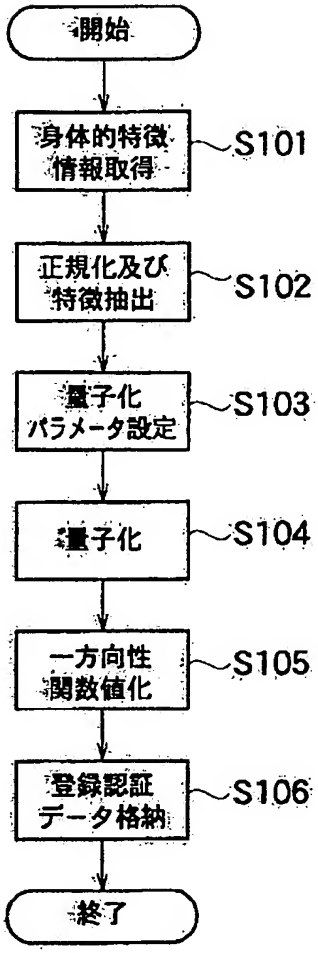
【図6】


認証結果格納部
15
照合部
7
判定回路
75
比較回路
73
登録認証データ格納部
11
一方向性関数値化回路
71
復号回路
77
特徴量子化部
3

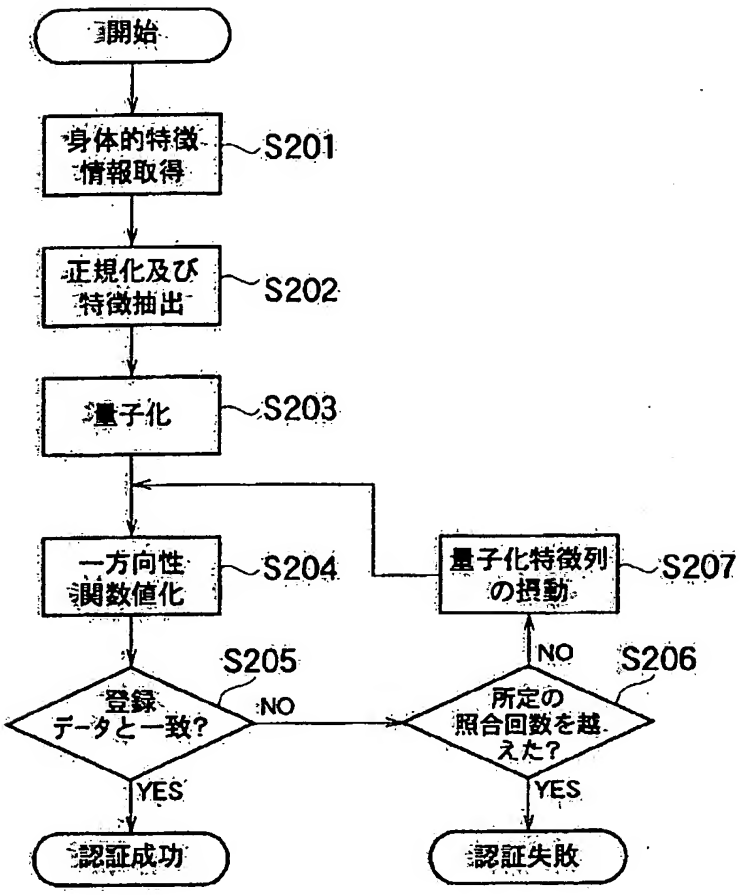
【図１０】


9
13
5
量子化パラメータ格納部
量子化パラメータ更新部
登録認証データ更新部
1
3
7
11
身体的特徴情報入力部
特徴量子化部
照合部
登録認証データ格納部
17
15
鍵生成部
認証結果格納部

【図１１】



【図１２】



フロントページの続き

(72)発明者　伴野　明
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　若原　徹
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　坂村　健
東京都品川区大崎四丁目９番２号

Ｆターム(参考)　5B043 AA09 BA06 EA04 EA05 FA07 FA09 GA04
5J104 AA07 KA01 KA03 KA06 KA16 NA11 PA14